iTrust Times

A Quarterly Newsletter

Issue Highlights:

Apr — Jun 2023 | Volume 9 Issue 2

From Centre Director's Desk

Celebrating 10 Years

Dear readers,

Greetings from iTrust!

I'm pleased to share that the Cyber Security Agency of Singapore has renewed the National Satellite of Excellence (NSoE) programme for another three years. Phase II of NSoE started in April this year and focuses on the development of technologies that can be rapidly transferred to the industry in four domains, namely, electric power, IoT, maritime, and water.

Trust has made new inroads internationally during the April-June quarter. Locked Shields 2023, the world's largest cyber-exercise held in Estonia, adopted a new digital twin developed by iTrust, namely, GASP (for Gas Processing). This twin was designed, built and configured in a record 4-months from iTrust's one-of-a-kind reconfigurable digital twin code base. GASP includes gas extraction, 3-stage compression, transmission, single-stage re-compression, and distribution. Across the Atlantic in Buford, Georgia, USA, iTrust demonstrated its advanced anomaly detection technologies during the Demo Day at The Water Tower (TWT). This was the first time that a team of iTrust researchers synchronised themselves across USA and Asia to launch attacks on the SWaT testbed in Singapore while displaying the impact, anomaly detection, and state visualisation in Buford. iTrust is currently contemplating setting up its own laboratory at the TWT for use by its partners and researchers in the USA. The National Cybersecurity R&D International Advisory Panel visited iTrust on April 11. The panel members were offered a glimpse into technologies developed by iTrust researchers and toured the testbeds. iTrust also hosted Dr Victor Bolbot from Aalto University and Dr Marina Krotofil, who delivered talks on, respectively, autonomous ships and cyber warfare.

iTrust continues to expand its outreach programme to secondary schools in Singapore. Andy Tay and Francisco Furtado are leading this programme where students from secondary schools undergo a cyber-security awareness programme. Siddhant Shrivastava is developing GURU, a specialised version of the SWaT digital twin. GURU is expected to be a flagship iTrust product for use in OT-related education and training.

Formally launched in 2013, iTrust is now celebrating its 10th anniversary. At the time of this writing, iTrust has provided direct assistance to over 4,000 researchers and industries across 83 nations through the provisioning of advanced datasets, internships, and unique opportunities to develop and evaluate their ideas and technologies. Today iTrust is widely recognised as a leading centre for

research in critical infrastructure security.

This is the last newsletter for which I am writing a forward. I will cherish the wonderful time and memories I have had working with the many researchers, staff, and faculty across Singapore, and internationally since 2013. I am happy to inform you that starting August 1, 2023, iTrust management will be in the able hands of new centre director Professor Jianying Zhou. I wish Professor Zhou the very best for success in maintaining the momentum that has led to innovation and service to the international research and industrial community.

I thank Mark Goh and iTrust staff who made this newsletter a continuous feature. My sincere thanks to the many people, especially at the Cyber Security Agency, Ministry of Defence, National Research Foundation, PUB Energy Market Authority, and the management of SUTD, whose trust and support have made iTrust possible.

Happy reading and best wishes to all readers of iTrust Times for a productive and happy 2023!

Aditya Mathur
Centre Director, iTrust, SUTD
Director, National Satellite of Excellence DeST-SCI
Professor Emeritus, Computer Science, Purdue University

News

NSoE Phase II

iTrust is proud to announce that it has received $14.4M in funds from the Cyber Security Agency of Singapore (CSA) for the second phase of the National Satellite of Excellence in Design Science and Technology for Secure Critical Infrastructure (NSoEDeST-SCI.) Phase II is set to enhance Singapore's status as a global leader in secure Critical Infrastructure design. By generating and demonstrating advanced technologies, validated in testbeds, and piloting them in operational plants, new business prospects will arise for iTrust staff, faculty, and students.

Phase II will build upon the research outcomes of the previous phase, with emphasis on enhancing the scalability and robustness of existing tools. Additionally, new methods and prototypes will be developed to broaden the capabilities encompassing the entire OT security pipeline, including prevention, detection, response, and recovery. This approach sets iTrust apart from current commercial offerings, making it distinct and unique in its contributions to the field.

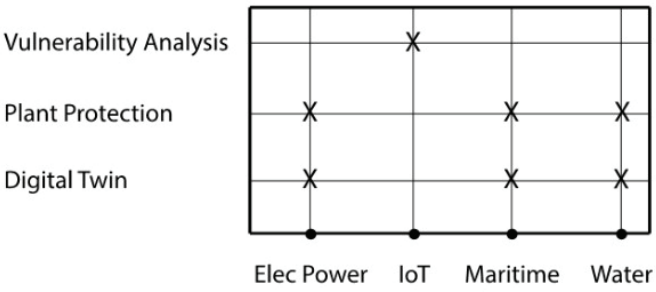

Fig 1: Phase II domains & focus areas

NSoE Phase II has been developed through discussions with the sector leads and co-leads and with the R&D partners. This led to the co-development of each sector's scope, work packages, objectives and deliverables. These partners include ABS, ADSC, DSO, MINDEF, MPA, Pacific Light Power, Power Automation, Resync Technologies, and PUB.

NSoE Phase II Work Packages, Sector Leads and Industry Partners:

Energy Sector
Binbin Chen

- *Scalable Digital Twin*
- *Collect Threat Intelligence*
- *Digitalisation of Energy Sector*
- *Software Patch Management*

IoT Sector
Sudipta Chattopadhyay

- *Monitoring IoT System Properties*
- *Generation of Malformed Communication*
- *Directed Communication Fuzzing*
- *Network-based Anomaly Detection*
- *Automated Malware Analysis*
- *IoT Threat Assessment*

Maritime Sector
Jianying Zhou

- *Fuzzing Shipboard OT Systems Communication*
- *Automated Exploit Creation*
- *Develop Software Cryptographic Library*
- *Use of Software Cryptographic Library*
- *Fingerprinting-based Device Authentication*
- *Multi-level Sensor Consensus-based Trust*
- *Create Multi-physics Virtual Models*
- *Develop list of Attack Scenarios*
- *Connection to Actual Testbed*

Water Sector
Aditya Mathur

- *Anomaly Detection in Water Supply Network*
- *Automated Response to Cyber Alerts*
- *Create Equipment Fault Library*
- *Advanced Digital Twin*

Key Events

Exercise Locked Shields 2023

Strong Collaboration Is Key To Effective Cyber Defense

Locked Shields 2023, an annual cyber defense exercise organised by NATO CCDCOE, was the most competitive and successful exercise to date. The exercise saw a big jump in quality among Blue Teams, with effective teams fostering strong collaboration between their strategic decision-makers and technicians to address all elements of a large-scale cyber-attack.

Mart Noorma, the Director of NATO CCDCOE, expressed his gratitude to all the Blue Teams, stressing the vital role they play in making Locked Shields the unique exercise it is. "The fact that more and more nations are joining shows the quality and value of Locked Shields. Thanks to our partners, we can offer the training audiences new technical challenges and new avenues to explore. Learning to tackle new opposition, adapt, and collaborate are the main aims of Locked Shields."

The Sweden-Iceland joint team emerged as the most effective participant in the exercise, followed by the Estonia-USA joint team and the Polish team. The 24 participating teams gained valuable and relevant training experience from Locked Shields, which offers a unique opportunity for teams to test their skills in a safe environment.

Carry Kangur, Head of the Exercise, noted that each of the participating teams could be regarded as winners as they will have gained valuable experience. "I know many people want to know who comes out on top. Even though scoring is a big part of the exercise, for us, it is more important to see participants adding new members and nations into their teams. It might sound like a cliché, but everybody is a winner at Locked Shields."

Locked Shields is an essential training exercise designed to test and improve the preparedness of member nations and partners against large-scale cyber-attacks. It remains a growing and developing exercise, and the organizers are continually adapting to offer new technical challenges and avenues to explore for the participants.

Article credits: The NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE

Demo at The Water Tower

In the course of conducting applied R&D to protect critical infrastructure, iTrust has developed two key technologies that have the most traction. The first is the SWaT digital twin, which, unlike traditional digital twins that are used mainly for predictive maintenance and system upgrades testing, is purpose-built for cyber activities such as training, education and cyber exercises,. The twin allows cyber attacks to be launched on it. It also includes AICrit (see article above), that has been licensed to SafeKrit, a US-based company which will pilot and market the technology in North America.

At the Demo Day organised by the Water Tower – an innovation hub focused on advancing the water industry – in Buford, Georgia, on 22 Apr, Prof Aditya Mathur and Research Associate Siddhant Shrivastava presented and gave a demonstration of the SWaT digital twin and AICrit to water technology companies and manufacturers, consulting and engineering firms, and water utilities. A team here at iTrust also provided onsite support during the demonstration so that the full capabilities of both technologies could be showcased. The presentations invited many queries from the curious and interested audience, and gave them much fruit for thought on what they needed to do to protect their plants and assets.

Fig 2: (From top left, clockwise): Aditya explaining the technology behind AICrit, Siddhant showing a demo of and presenting the SWaT Digital twin

Visits

UN-Singapore Cyber Fellowship

On 12 May, iTrust hosted participants of the UN-Singapore Cyber Fellowship. During this site visit, iTrust Co-centre Director Prof Zhou Jianying, Cyber Tech Lead Francisco Furtado and Cyber Security Technology Engineer Tay Boon Kiat gave a tour of our facilities - the Secure Water Treatment (SWaT) and Electric Power and Intelligent Control (EPIC) testbeds.

Fig 3: Prof Zhou introducing iTrust to the UN-SIngapore Cyber Fellows.

The Fellows witnessed firsthand the potential repercussions and harm that attacks on Operational Technology (OT) systems can cause. The Fellows also engaged in a comprehensive Tabletop Exercise (TTX) centred around an OT attack scenario. The session was concluded with a simulated press conference.

Fig 4: The Fellows engaging in the TTX.

Photo credits: ASEAN-Singapore Cybersecurity Centre of Excellence

National Cybersecurity R&D Programme (NCRP) International Advisory Panel (IAP)

The Cyber Security Agency of Singapore (CSA) organised a visit for the National Cybersecurity R&D Programme (NCRP) International Advisory Panel (IAP) to iTrust and the Future Communications Research & Development Programme (FCP) office on 11 Apr. The IAP comprises prominent local and international cybersecurity practitioners to help Singapore chart its

Fig 5: Francisco Furtado (Cyber Tech Lead; second from left) giving a testbed tour to IAP members (from left) Ms Mihoko Matsubara (Chief Cybersecurity Strategist, NTT Corporation), Ms Yong Ying-I (Senior Advisor, Ministry of Communications and Information), Mr Tan Peng Yam (Chief Defence Scientist, Ministry of Defence), Mr Khoo Boon Hui, (Board Director, Ensign InfoSecurity), and Prof Isaac Ben-Israel (Director, Blavatnik Interdisciplinary Cyber Research Centre, Tel Aviv University)

next steps in cybersecurity R&D strategies and policies. To do so, they were briefed on the respective centres' achievements and recent developments in cyber security by iTrust Assistant Director Mark Goh and FCP Deputy Director Assoc Prof Binbin Chen. Their visit was wrapped up with a demo by Prof Chen's team and a tour of iTrust's testbeds.

Public Lectures

Kinetic- and Cyber Warfare:

Twins, siblings, or distant relatives? Or why bombs speak louder than electronic bits?

After a long hiatus, iTrust welcomed back Dr Marina Krotofil to conduct a public lecture on Cyberwarfare on 10 May 2023. Dr Krotofil is a seasoned cybersecurity expert with extensive hands-on experience safeguarding Industrial Control Systems (ICS) and Industrial Internet of Things (IIoT).

Fig 6: Prof Zhou introducing Dr Marina to the attendees.

In her talk, Dr Krotofil defined hybrid war as a combination of kinetic and cyber warfare. This limited perspective, lacking real-world examples of hybrid war until recently, led to her argument that cyberwarfare, particularly attacks on critical infrastructures, could play a crucial role during significant conflicts involving combat actions. However, recent events in the war in Ukraine had demonstrated a preference for kinetic weapons during tactical military operations. She questioned the audience: Have you ever wondered why this preference exists?

Dr Krotofil delved deeper into the complexities of cyber-physical attacks, allowing the audience to gain a better understanding of why cyber-attacks on critical infrastructures tended to be more opportunistic than strategic and may not always achieve the desired impact. Drawing from her firsthand experiences, Dr Krotofil elaborated and explored the various factors influencing the success of cyber-physical operations and elucidated the role of such attacks in both war and peace times, interlacing them with real-life examples and case studies. Finally, Dr Krotofil also addressed the recent disclosure of top-secret Russian documents concerning extensive cyber security programmes, offering insights into the future of hybrid warfare.

Fig 7: (from left) Dr Awais Yousaf, Li Meixuan, Mark Goh, Prof Jianying Zhou, Francisco Furtado, Dr Marina Krotofil, Sean Gunawan, Ivan Christian.

Safety and Cybersecurity in Autonomous Ships

Dr Victor Bolbot, a postdoctoral researcher at the Research group on Safe and Efficient Marine Systems of Aalto University, was in SUTD to shed light on the crucial aspects of safety and cybersecurity in autonomous ships by answering two key questions: How does the ever-evolving world of cybersecurity in maritime transport look like? What is the cutting-edge technology behind autonomous ships and the safety measures that are put in place?

Fig 8: Prof Zhou introducing Dr Bolbot to the attendees.

Autonomous ship projects have gained traction worldwide, with numerous prototypes already deployed. Dr Bolbot gave an enlightening presentation where the attendees explored the historical evolution

of autonomous ships, fundamental components that made autonomous ships possible, the expected benefits that autonomous ships bring to the table, the challenges associated with the introduction of autonomous ships, with a specific emphasis on safety and cybersecurity, as well as the potential future advancements in autonomous ships and ongoing research, with a strong focus on safety and cybersecurity. Dr Bolbot also shared about Aalto University's research initiatives related to autonomous ships.

Dr Bolbot holds a doctoral degree from the University of Strathclyde in Glasgow, Scotland, as well as a master's degree from the National Technical University of Athens in Greece.

Outreach

Yusof Ishak Secondary School Cyber Wellness Week

As Singapore marches towards digitalisation, the education sector has increasingly adopted e-learning, augmented with smart devices. It is therefore crucial that students are also prepared with the right skills and knowledge to use these devices responsibly and safely.

Fig 9: Andy speaking to students about cyber wellness.

In May 2023, iTrust was invited to Yusof Ishak Secondary School for its Cyber Wellness week with the goal of empowering students and enhancing their understanding of cybersecurity risks associated with social media platforms and mobile phones. Cyber Tech Lead Francisco Furtado and Research Assistant Andy Tay were at the school to conduct two such sessions. Each session accommodated 40 students and focused specifically on social media and mobile phone security. The sessions' primary objective was to educate and familiarise students with the potential security threats that can arise from using different social media platforms and smart devices.

To bring home the message, they shared a case study of a fellow researcher who encountered a security breach that led to her immediately being logged out from both her Instagram and Facebook accounts within a span of five minutes, and her WhatsApp account 30 minutes later. Another case they shared was of a woman who unknowingly scanned a QR code embedded with malware. Francisco and Andy then walked through with the students the steps that the hacker took, so as to illustrate how cybercriminals can exploit vulnerabilities – from points of entry to gaining access – present in the Internet and on our devices.

Francisco and Andy wrapped up the sessions by encouraging the students to place a strong focus on practical strategies to safeguard their personal devices and information against potential vulnerabilities.

Internships

AICrit IT L1

By Caven Chew

Critical infrastructure systems employ communication protocols that are distinct from conventional IT systems. In particular, OT networks lack a standardised protocol; there may be variations in protocols across different manufacturers and versions of PLCs. Consequently, traditional Intrusion Detection Systems (IDS) cannot be deployed to effectively detect potential security breaches on the SCADA network.

To address this challenge, I undertook the development of AICrit L1, a real-time IDS for iTrust's SWaT (Secure Water Treatment) testbed that is specifically designed to identify attacks targeting PLCs, by analysing packets directed towards them.

Given that thousands of packets are transmitted every second in an OT network, (estimated to be around 12,000 packets per second), the real-time application I developed is optimised for speed and efficiency. I frequently reviewed and optimised the programme to enhance its efficiency, honing my programming skills and knowledge of programme optimisation in the process.

During my internship at iTrust, I gained valuable insights into the mechanisms used to control devices within OT networks, as well as the specifics of the structure and contents of packets within SWaT. I managed to complete and test the programme against attacks

launched on the testbed.

By Ng Guo Feng Eric

At iTrust, I had the opportunity to collaborate with Dr Gauthama Raman to improve AICrit-IT, a multi-level Intrusion Detection System (IDS) designed to protect the OT systems against malicious attacks. Our primary goal was to examine network packet decoding and automated network detection in order to develop more effective solutions for identifying attacks on the industrial control systems (ICS).

ICS are at risk of significant damage if attackers can gain access to the system and modify the PLCs using custom malicious scripts and network packets that change tag values. This can lead to equipment failure and safety risks, making it essential that an IDS can detect these attacks before they cause harm.

AICrit is designed to optimise network traffic sniffing, decode packets in real-time, and reflect any anomalies in the data being sent over the network. Through our work on this project, I gained a wealth of experience in analysing network packets through deep packet layer inspection and decoding them into readable content, enabling AICrit to determine whether the network behaviour is normal.

Overall, the development of AICrit-IT was a challenging and rewarding experience that allowed me to deepen my knowledge of network security and contribute to the development of a critical tool for safeguarding ICS against cyberattacks.

PyDNP3Twin

By Eden Siew

During my internship in iTrust, I worked on PyDNP3Twin – the implementation of Distributed Network Protocol 3 (DNP3) as a communications protocol in the SWaT Digital Twin. For this project, I was guided by Prof Aditya, who created the SWaT Digital Twin, and Francisco, the developer who implemented the existing communications protocol in the Digital Twin – Open Platform Communications Unified Architecture (OPC UA).

Through the project, I learnt how different Operational Technology (OT) devices communicate in the Digital Twin, and the inner workings of protocols used in the Digital Twin. OT protocols are a niche area and lack the support of an online community which made the project challenging. Through trial and error I improved my understanding of DNP3, which made the implementation process smoother.

While working on the project, I was able to hone my Python skills, by deciphering and writing my own implementation of existing functions. This has allowed me to make great strides in my progress in the project and gave me a deeper understanding of the various libraries used.

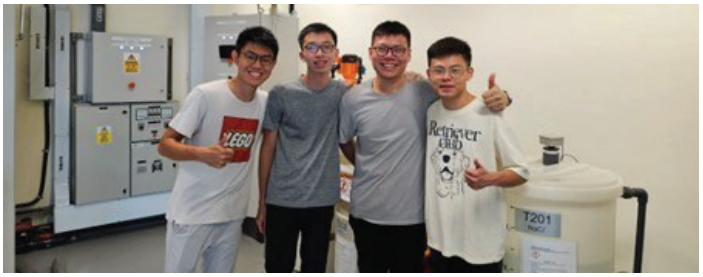

Fig 10: Interns (from left) Roderick Kong, Eden Siew, Caven Chew, Eric Ng.

AutoOTViz: OT Dashboard Automation

By Roderick Kong

Throughout my internship at iTrust, I have been working closely with Dr Gauthama Raman to develop AutoOTViz – an automated OT visualiser that graphically displays information about the status of cyber-physical systems. In AutoOTViz, colourful visual panels such as graphs and gauges are used to represent plant data such as pressure and rate of flow of the OT plant, and anomalies detected during its operation. The dashboard provides an overview of the plant's trends, as well as any abnormalities. AutoOTViz builds on the idea of OT Vision, an earlier technology also developed by an intern with a similar purpose, by automating the manual process of creating the dashboards.

With the advent of dashboards such as Code, it has become possible to write and run programming scripts to generate dashboards using existing monitoring solutions. I leveraged on the dashboard-as-code capabilities of Grafana (an open-source analytics and monitoring tool) to create AutoOTViz and designed it to be as dynamic as possible. Using AutoOTViz, analytics dashboards can be created instantly for any current or future digital twins. Hence, this project simplifies the implementation of dashboard monitoring

solutions for critical information infrastructures.

While developing AutoOTViz, I gained valuable experience in programming and knowledge on cyber-physical systems. I learnt to utilise and implement existing technologies using APIs, and worked with time series databases, specifically, InfluxDB. I am grateful for the opportunity to work alongside Dr Raman to develop AutoOTViz.

Openstack

By Jadon Lee Jun Jie

In my six months of interning at iTrust, I have set up a service known as Openstack on two servers that were provided to me to automate, increase scalability, and improve the efficiency of provisioning and managing iTrust's Virtual Machines. Openstack is a free and open -source software for cloud computing providing infrastructure-as-a-service (IAAS) which allows for the management and automation of deployment of Virtual Machines. As my course in Temasek Poly was in Cyber Security and Digital Forensics. I have also ensured that my Openstack includes security controls to ensure the basic and continued security of the environment. Currently, I am employed as a Research Technician and have been tasked to help out for CISS 2023 by setting up the IP cameras. I am also tasked to support research experimentation and engineering, as well as helping to maintain and support the iTrust infrastructure such as the firewall and NAS servers, coordinate Testbed safety, maintenance and upgrade.

LinkedIn

iTrust is now on LinkedIn — connect with us! Feel free to reach out to us to explore research collaborations, testbed usage and training and testing services.

General Enquiries

iTrust: *itrust*
NSoE: *nsoe_destsci*
CiMS: *cims*

Management

Prof. Aditya P MATHUR
Centre Director, iTrust
Director, National Satellite of Excellence, DeST-SCI
Professor Emeritus, Computer Science, Purdue University
aditya_mathur

Prof. Jianying ZHOU
Co-Centre Director, iTrust
Professor, Information Systems Technology and Design
jianying_zhou

Francisco FURTADO
Cyber Tech Lead, iTrust
francisco_dos

Mark GOH
Assistant Director, iTrust
mark_goh

iTrust Laboratories

Andrew TAY
Research Senior Technologist
andrew_taykongngee

TAY Boon Kiat
Cyber Security Technology Engineer
boonkiat2_tay

Aanand R
Cyber Security Technology Engineer
Aanand_r

National Satellite of Excellence

Jillian CHIN
Manager
jillian_chin

Angie Ng
Manager
angie_ng

Siti Nadhirah Shaik NASAIR
Research Associate
siti_nadhirah

Vanessa LEE
Deputy Manager
vanessa_lee

Email addresses end with the domain ***@sutd.edu.sg***